Date de réception : 23/01/2015

Published ID	:	C-362/14
Document number	:	16
Register number	:	977302
Date of lodgment	:	06/11/2014
Date of entry in the register	:	06/11/2014
Type of document	:	Observations
	:	Document
Lodgment reference	:	DC33510
File number	:	1
Person lodging document	:	Anthony Joyce Irlande

In the Court of Justice of the European Union

Case C-362/14

Maximillian Schrems

Applicant

-and-

Data Protection Commissioner

Defendant

WRITTEN OBSERVATIONS OF IRELAND

Submitted by Eileen Creedon, Chief State Solicitor, Osmond House, Little Ship Street, Dublin 8, acting as Agent, accepting service via e-Curia with an address for service at the Embassy of Ireland, 28 route d'Arlon, Luxembourg, assisted by David Fennelly BL of the Bar of Ireland.

Ireland has the honour to submit written observations in these proceedings, the subject of a reference for preliminary ruling from the High Court (Ireland) made on 25 July 2014.

Dated the 6th day of November 2014

A. Introduction

1. Ireland submits these Written Observations pursuant to Article 23 of the Protocol on the Statute of the Court of Justice of the European Union.

2. The High Court of Ireland ("**the referring court**") has referred two questions to the Court of Justice of the European Union for preliminary ruling ("**the Reference**") under Article 267 of the Treaty on the Functioning of the European Union ("**TFEU**"). By its first question, the High Court asks whether, in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) (**"the Commission Decision**") having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union, the provisions of Article 25(6) of Directive 95/46/EC (**"the Directive**") notwithstanding. By its second question, which is posed in the alternative, the High Court asks whether the office holder may and/or must conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published.

3. As the circumstances in which the questions arise have been set out in detail in the Reference and in the Judgment of the High Court delivered on 18th June 2014, it is not proposed to address the circumstances underlying the Reference in detail save insofar as they arise in considering the substantive issues.

B. Preliminary Observations

4. Before addressing the substantive issues raised in the Reference, Ireland considers it appropriate to make a number of preliminary observations.

(i) No Challenge to the Validity of the Directive, the Commission Decision or the Irish implementing legislation

5. First, it must be emphasized that, in the national proceedings, there is no challenge to the validity of the Directive, the Commission Decision or the Irish implementing legislation, the Data Protection Acts 1988-2003 ("**the Data Protection Acts**").

6. While the referring court has expressed certain views on the compatibility *in abstracto* of the Commission Decision with the Charter of Fundamental Rights ("**the Charter**"), the referring court itself emphasises that neither the validity of the Directive nor the Commission Decision has been challenged in the national proceedings.[1] In the absence of any finding of invalidity by this Court, Ireland considers the Directive and the Commission Decision to be valid and binding on Member States. In this case, there has not been any direct challenge to the validity of those acts and there has not been argument and submissions on this point by the parties before the referring court. In the circumstances, Ireland considers that examination of the validity of the Directive and/or the Commission Decision should await a case in which the question of validity is directly in issue in, and necessary for the resolution of, the national proceedings and in which the referring court has had the benefit of argument and submissions from the parties on this question.

7. For these reasons, while Ireland will make a number of general observations in relation to the validity of the Commission Decision, the focus of these observations is on the proper interpretation of the Directive and the Commission Decision. In the event that the Court proposes to examine the validity of the Directive or the Commission Decision as such, Ireland reserves the right to make further submissions to the Court on these issues.

[1] Reference, paragraphs 20 and 25.

8. As the referring court has also made clear in the Reference, there is no suggestion that Irish law, and specifically the implementing legislation (the Data Protection Acts), does not reflect the terms of the Directive and/or the Commission Decision.[2]

9. While the questions before the Court raise issues of European Union law, those issues are closely connected with issues of Irish law, notably the scope and limits of the Data Protection Commissioner's investigative powers under the Data Protection Acts. In particular, the manner in which the Data Protection Commissioner carries out investigations or otherwise exercises its investigative powers is primarily a matter of Irish law. In considering the questions referred, it is thus important to distinguish clearly between the issues of European Union law and issues of Irish law.

(ii) Independence of the Data Protection Commissioner as a matter of Irish law

10. Secondly, it must be emphasized that the Data Protection Commissioner ("**the Commissioner**"), whose decision is at issue in the national proceedings, is entirely independent as a matter of Irish law.

11. Article 28(1) of the Directive provides that each Member State "shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive". It further states that these authorities "shall act with complete independence in exercising the functions entrusted to them". Article 28(3) specifically provides that each such authority shall have powers to carry out its functions, including "investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties". Article 28(4) states that each supervisory authority "shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data".

[2] Reference, paragraph 20.

12. Under section 9(1C) and 9(3) of the Data Protection Acts, the Data Protection Commissioner is designated as the supervisory authority in the State for the purposes of the Directive. Section 9(2) provides that the provisions of the Second Schedule to the Acts shall have effect in relation to the Commissioner. Paragraph 1 of the Second Schedule provides that the Commissioner "shall be a body corporate and shall be independent in the performance of his functions". Thus, the Commissioner enjoys an express statutory guarantee of independence in Ireland in the performance of his/her functions.

13. This independence extends to the manner in which the Data Protection Commissioner carries out the investigative and enforcement functions under the Data Protection Acts. While the Commissioner must at all times act in accordance with the Data Protection Acts and with applicable EU law, the Commissioner enjoys a significant amount of discretion in how he or she conducts its investigations under section 10 of the Data Protection Acts, one of the core provisions at issue in the national proceedings. Under section 10(1)(a), the Commissioner "*may* investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention".[3] Thus, section 10(1)(a) envisages two categories of investigation: an investigation on foot of a complaint by an individual; an investigation of the Commissioner's own motion. In case of a complaint by an individual, section 10(1)(b) provides that the Commissioner "shall" do the following: (i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and (ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification. It follows that, unless the Commissioner is of the opinion that the complaint is frivolous or

[3] Emphasis added.

vexatious, the Commissioner must investigate the complaint and, in default of an amicable resolution, notify the complainant of his or her decision in relation to the complaint. If the Commissioner considers the complaint frivolous or vexatious, however, the Commissioner is not under any duty to investigate the complaint. In addition, under section 10(1A), the Commissioner "may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof". If, on foot of an investigation, the Commissioner is of the view that there is a contravention of the Data Protection Acts, the Commissioner may take enforcement measures, which are specified in the remainder of section 10.

14. While, in addressing the questions before the Court, Ireland will express its views on the proper interpretation of the Data Protection Acts in light of EU law, it does so with full respect for the independence of the Data Protection Commissioner in the exercise of its investigative and enforcement functions under the Data Protection Acts.

C. The Questions Referred

(i) Introduction

15. Chapter IV of the Directive addresses the transfer of personal data to third countries. Under Article 25(1) of the Directive, Member States shall provide that such a transfer may take place "only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection". Under Article 25(6), the Commission may find, by way of decision under Article 31(2), that a "third country ensures an adequate level of protection" and Member States shall take the measures necessary to comply with the Commission's decision. The Commission Decision at issue in these proceedings is a "decision" for the purposes of Article 25(6). Under the mechanism provided for in the Decision, organisations wishing to transfer data to the United States self-certify for compliance with the Safe Harbour Privacy Principles, annexed to the Decision, publicly

disclose their privacy policies, and are subject to the jurisdiction of the Federal Trade Commission and the US Department of Transportation.

16. Notwithstanding the existence of the Commission Decision, the Applicant in the national proceedings has complained to the Data Protection Commissioner that transfers of personal data by Facebook Ireland Limited to its parent company in the United States, Facebook Inc., do not ensure adequate protection for the data subject, particularly insofar as access to such data by the United States authorities, in particular the National Security Agency, is concerned. The Data Protection Commissioner invoked the power not to investigate the complaint on the grounds that it was frivolous or vexatious in the sense that it was unsustainable in law.[4] The Applicant has challenged this decision by way of judicial review in the national proceedings.

17. The first question posed by the referring court asks in essence whether, in such circumstances, having regard to Articles 7, 8 and 47 of the Charter, and notwithstanding Article 25(6) of the Directive, an independent office holder, such as the Data Protection Commissioner in Ireland, is "absolutely bound" by the Commission Decision. The second question posed by the referring court is whether an office holder such as the Data Protection Commissioner may and/or must conduct his or her own investigation of the matter in light of factual developments since the publication of the Commission Decision.

18. When the questions are considered together in light of the Reference as a whole, it is submitted that the phrase "absolutely bound" used in the first question may give rise to some confusion. Ireland's view is that the Data Protection Commissioner is indeed bound by the Commission Decision. However, the binding effect of the Decision – understood in light of the Directive and indeed the Charter of Fundamental Rights insofar as it is relevant – is not such as to preclude all investigations by the Data Protection Commissioner into complaints that transfers of data to the United States under the

[4] In relation to the term "frivolous and vexatious", the referring court notes, at paragraph 4 of the Reference, that "[as] a matter of Irish law and in this particular statutory context these words simply mean that the Commissioner concluded the claim was unsustainable in law", referring further to paragraphs 34 - 40 of the Court's Judgment delivered on 18th June 2014.

Commission Decision do not ensure adequate protection for the data subject or indeed is not such as to require all such complaints to be dismissed *in limine*, that is, as a preliminary matter without any consideration of the merits of the complaint.

(ii) The Binding Character of the Commission Decision

19. Article 25(6) of the Directive provides that, in circumstances where the Commission has made a finding that a third country ensures an adequate level of protection in accordance with the procedure referred to in Article 31(2), "Member States shall take the measures necessary to comply with the Commission's decision". The Commission Decision itself provides, at Article 5, that Member States "shall take all the measures necessary to comply with this Decision at the latest at the end of a period of 90 days from the date of its notification to the Member States". Article 6 confirms that the Decision "is addressed to the Member States". While the Decision is addressed to the Member States, the duty on Member States to take the necessary measures to comply includes measures to ensure compliance with the Decision within Member States.

20. Ireland has given effect to the Commission Decision in section 11 of the Data Protection Acts. First, section 11(2)(a) of the Data Protection Acts provides that, where a question arises in any proceedings under the Acts about the adequacy of protection in a third country and a Community finding has been made in relation to such transfers, the question "shall be determined in accordance with that finding". Secondly, section 11(4)(c) of the Data Protection Acts provides that the Commissioner "shall comply with any decision of the European Commission under the procedure laid down in Article 31.2 of the Directive made for the purposes of paragraph 3 or 4 of Article 26 of the Directive". It follows that, where issues falling within the scope of the Commission Decision arise before either the Data Protection Commissioner or the Irish courts, the Decision clearly binds the Commissioner and/or the courts.

21. It is thus clear that the Commission Decision is binding on the Data Protection Commissioner.

(iii) The Effect of the Commission Decision on Investigations by the Data Protection Commissioner

22. While it is clear that the Commission Decision is binding on the Data Protection Commissioner, Ireland submits that the binding effect of the Commission Decision is not such as to preclude all investigations by the Data Protection Commissioner into complaints that transfers of data to the United States under the Commission Decision do not ensure adequate protection for the data subject. In particular, the binding effect of the Commission Decision does not require that all such complaints be dismissed *in limine*; indeed, in appropriate cases, the provisions of the Commission Decision may exclude the possibility of a complaint being dismissed *in limine*. This is clear from an analysis of the terms of the Directive and the Commission Decision and the scheme that they combine to create.

23. Insofar as the Directive is concerned, Article 25 is the relevant provision addressing the transfer of personal data to third countries. As set out above, Article 25(1) lays down the core principle that personal data may be transferred to third countries "only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection." Article 25(2) sets out in some detail how the concept of adequate level of protection should be assessed: this assessment is a holistic one, which takes place "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country". Under Article 25(3), the Member States and the

Commission "shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2".[5]

24. The remaining provisions of Article 25 deal with Commission findings under a procedure provided for in Article 31(2) of the Directive. Under Article 25(4), the Commission may find that a third country does not ensure an adequate level of protection for transfers of personal data, in which case Member States "shall take the measures necessary to prevent any transfer of data of the same type to the third country in question". In the event of such a finding, Article 25(5) envisages the Commission, at the appropriate time, entering into negotiations "with a view to remedying the situation". Under Article 25(6), the Commission may find that a third country ensures an adequate level of protection for transfers of personal data, in which case Member States "shall take the measures necessary to comply with the Commission's decision".

25. As discussed above, the Commission Decision at issue in this case is a "decision" within the meaning of Article 25(6). Article 1 of the Decision provides that, for activities falling within the scope of the Directive, the Safe Harbour Privacy Principles (contained in Annex I of the Decision and implemented in accordance with the guidance of the US Department of Commerce contained in Annex II) "are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States". The documents annexed to the Decision – composed of the Principles, a series of FAQs, an enforcement overview, and certain correspondence from US government bodies – form the basis for the Safe Harbour system, a system of voluntary self-certification by organisations that they adhere to, and properly implement, the Principles and that subjects those organisations to the jurisdiction of the Federal Trade Commission and the US Department of Transportation.

[5] Section 11(3) of the Data Protection Acts provides that the Commissioner "shall inform the Commission and the supervisory authorities of the other Member States of any case where he or she considers that a country or territory outside the European Economic Area does not ensure the adequate level of protection referred to in subsection (1) of this section".

26. Article 2 of the Decision confirms that the Decision "concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof". Recital (6) to the Decision also notes that sectors and/or data processing "not subject to the jurisdiction of any of the government bodies in the United States listed in Annex VII to this Decision" – that is, the Federal Trade Commission and the US Department of Transportation – should fall outside the scope of this Decision. Thus, the Commission Decision is limited in its scope and only applies to transfers of personal data and activities provided for therein.

27. Having regard to Articles 1 and 2 of the Decision, there may well be circumstances in which a complaint of inadequate protection in respect of personal data transferred to the United States raises issues about the scope and applicability of the Commission Decision. In appropriate cases, a competent authority, such as the Data Protection Commissioner, may need to investigate a complaint in order to determine whether or not it falls within the scope of the Commission Decision.

28. Article 3(1), which is "without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC", provides that the competent authorities in Member States "may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data" in two cases:

    (a) where "the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs"; or

(b) where "there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond".

While the exercise of the power to suspend data flows is itself subject to relatively strict limits, Article 3 constitutes an important safeguard mechanism enabling competent authorities, such as the Data Protection Commissioner, to intervene notwithstanding the apparent applicability of the Commission Decision.

29. Article 3(1) thus limits the binding effect of the Commission Decision. Because Article 3(1) specifically provides for circumstances in which the operation of the Safe Harbour system may have to be suspended, a competent authority, such as the Data Protection Commissioner, would be required to investigate a complaint of inadequate protection in such circumstances, notwithstanding the apparent applicability of the Commission Decision. If the competent authority concludes that the requirements of Article 3(1) are satisfied, it may exercise its existing powers to suspend data flows to an organisation that has self-certified under the Safe Harbour system. In conducting its investigation under this provision, the Commissioner may have regard to factual developments which have taken place since the Commission Decision was first published.

30. While it is by no means clear that the conditions for suspension set out in Article 3(1)(b) of the Commission Decision would be satisfied on the facts of the present case,[6] dismissal of a complaint on jurisdictional grounds, as occurred in this case, would limit a competent authority's ability to assess the relevance of, and apply, Article 3(1). If the binding effect of the Commission Decision were such as to exclude *any* investigation into the adequacy of protection, this would prevent legitimate complaints based on Article 3(1) from being considered and determined by the competent authorities and would

[6] See in that regard paragraph 19 of the Reference.

undermine the practical effectiveness of this important safeguard enshrined within the Commission Decision.

31. The further provisions of Article 3 of the Commission Decision highlight the close cooperation between Member States and the Commission in respect of cases of possible non-compliance. Under Article 3(2), Member States shall inform the Commission without delay when measures are adopted on the basis of Article 3(1). Under Article 3(3), the Member States and the Commission "shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles… fails to secure such compliance". Under Article 3(4), if the information collected under the preceding paragraphs provides "evidence that any body responsible for ensuring compliance with the Principles…. in the United States is not effectively fulfilling its role, the Commission shall inform the Department of Commerce and, if necessary, present draft measures … with a view to reversing or suspending the present Decision or limiting its scope". These provisions complement Article 4 of the Decision which states that the Decision "may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation".[7] It also provides that the Commission shall in any case evaluate the implementation of the Decision "on the basis of available information" three years after its notification and report "any pertinent findings …including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection…". The review process enshrined in the Commission Decision thus ensures ongoing scrutiny of the operation of the Safe Harbour system.[8]

32. Looking at the scheme of the Directive and the Commission Decision as a whole in respect of transfers of personal data to the United States, it is submitted that compliance with the Commission Decision does not necessarily preclude all investigations on the part

[7] See also Recital (9) to the Commission Decision (providing that Safe Harbour "may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved").

[8] In this regard, it may be noted that there are ongoing negotiations between the European Union and the United States on the operation of the Safe Harbour system.

of the Data Protection Commissioner of a complaint by an individual about the adequacy of protection of data transfers to the third country and does not require that complaints of this kind are dismissed as a preliminary matter without any consideration of the merits. Indeed, in certain circumstances, for example where a complaint raises issues under Article 3(1)(b) of the Commission Decision, the Decision may exclude the possibility of a complaint being dismissed *in limine*. Thus, under the Directive and the Commission Decision, competent national authorities, such as the Commissioner, may play a limited but important supervisory role and provide independent scrutiny of transfers of personal data to the United States in appropriate cases.

33. It must be stressed that, subject to these considerations, the precise manner in which competent authorities, such as the Data Protection Commissioner, carry out their investigations and process individual complaints falls to be determined by national law.

34. For all these reasons, it is submitted that the Data Protection Commissioner, and any other independent office holder charged with similar functions, is bound by the Commission Decision in its determination of a complaint by an individual that the level of protection afforded by a third country in respect of which there is a Commission Decision is inadequate. However, it is submitted that the Data Protection Commissioner, and any other independent office holder charged with similar functions, *may* conduct an investigation into such a complaint in appropriate cases, in particular in cases falling within the scope of Article 3(1) of the Commission Decision.

(iv) The Relevance of the Charter of Fundamental Rights

35. In light of these conclusions, Ireland submits that it is possible to interpret the Directive and the Commission Decision in such a way that they do not preclude all investigations by national competent authorities, such as the Data Protection Commissioner, into the adequacy of protection afforded to transfers of personal data to third countries, such as the United States, which are the subject of decisions within the meaning of Article 25(6) of the Directive. Ireland also submits that, by interpreting the Directive and the

Commission Decision in this way, there is no conflict between the Directive and/or the Commission Decision and the Charter of Fundamental Rights and, in particular, Articles 7 and 8 thereof.

36. While the Directive and the Commission Decision both pre-date the entry into force of the Charter of Fundamental Rights under Article 6 of the Treaty on the European Union, the rights protected under Articles 7, 8 and 47 of the Charter, invoked by the referring court, were all protected under EU law prior to the entry into force of the Charter.[9] Nevertheless, it is clear that EU acts, such as the Directive and the Commission Decision, must now be interpreted in light of the Charter which has, under Article 6(1) TEU, "the same legal value as the Treaties".

37. Article 51 states that the provisions of the Charter are addressed to "the Member States only when they are implementing Union law". This Court has confirmed in *Åkerberg Fransson* that the Charter is "applicable in all situations governed by European Union law, but not outside such situations".[10] If legislation falls within the scope of European Union law, the Court, when requested to give a preliminary ruling, "must provide all the guidance as to interpretation needed in order for the national court to determine whether that legislation is compatible with the fundamental rights the observance of which the Court ensures".[11] It is clear that the transfer of personal data to third countries, such as the United States, may engage the Charter, including the right to privacy protected under Article 7 of the Charter and the protection of personal data under Article 8 of the Charter.[12] When Ireland is implementing the Directive and the Commission Decision, as in the instant proceedings, the protections of the Charter therefore apply.

---

[9] See the Explanations to the Charter, available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF (last accessed 3 November 2014).

[10] Judgment in *Åkerberg Fransson*, Case C-617/10, ECLI:EU:C:2013:105, paragraph 19.

[11] Judgment in *Åkerberg Fransson*, ECLI:EU:C:2013:105, paragraph 19.

[12] Judgment in *Digital Rights Ireland & Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

38. In Ireland's submission, the suggested interpretation of the Directive and the Commission Decision – in such a way that they do not preclude all investigations by national competent authorities, such as the Data Protection Commissioner, into the adequacy of protection afforded to transfers of personal data to third countries, such as the United States, which are the subject of decisions within the meaning of Article 25(6) of the Directive – is fully compatible with Articles 7, 8 and 47 of the Charter.

39. Without prejudice to this submission, and Ireland's earlier submission that examination of validity of the Directive and/or the Commission Decision should await a case in which it is directly in issue and has been fully argued, Ireland makes the following observations on the compatibility of the Directive and the Commission Decision with the provisions of the Charter:

(i) First, while the referring court has made extensive reference to the important judgment of this Court in *Digital Rights Ireland*, the issues in that case – which involved a challenge to the validity of the Data Retention Directive – were very different from those raised in these proceedings. Whereas the Data Retention Directive involved a derogation "from the system of protection of the right to privacy established by Directives 95/46 and 2002/58",[13] Article 25 of the Directive and the Commission Decision involve an extension of this system of protection of the right to privacy to transfers of personal data to third countries.

(ii) The extension of the Directive's system of protection to third countries, by its very nature, presents challenges. The EU and its Member States do not have jurisdiction under international law to unilaterally impose data protection rules on third countries.[14] As recital (3) to the Commission Decision illustrates, third countries may have very different methods of protecting data and privacy interests from those used within the EU. For these reasons, the EU and its Member States must engage and negotiate with third countries in order to reach agreement on an adequate level of

[13] Judgment in *Digital Rights Ireland & Others*, ECLI:EU:C:2014:238., paragraph 32.
[14] See e.g. Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013), Ch. 6.

protection for data transfers to those third countries under Article 25 of the Directive. In doing so, and in giving effect to any commitments flowing from such negotiations, the EU institutions and its Member States are subject to the duty of sincere cooperation.[15] Article 25 of the Directive does not require an identical or equivalent level of protection but rather it requires an "adequate level of protection"; thus, there may be circumstances in which a third country fails to protect a subject's data to precisely the same extent as under EU law but where the EU may nonetheless consider the protection adequate. Nevertheless, the Safe Harbour Privacy Principles contained in Annex I to the Commission Decision reflect the core principles of the Directive.

(iii) Insofar as Article 8 of the Charter specifically is concerned, it must be noted that the explanation to that provision states that it is based *inter alia* upon the Directive, which contains "conditions and limitations for the exercise of the right to the protection of personal data".[16] Under Article 6(1) TEU, the rights, freedoms and principles in the Charter shall be interpreted "with due regard to the explanations referred to in the Charter, that set out the sources of those provisions". Article 51(2) of the Charter provides that the Charter "does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties" while Article 52(2) of the Charter states that "[r]ights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties". In light of these provisions, it is submitted that the scope of Article 8 of the Charter must be understood in light of the conditions and limitations laid down in the Directive, including Article 25 thereof and the Commission Decision which has been concluded on foot of that provision. More

[15] Article 4.3 TEU. See, for example, Judgment in *Commission v. Greece*, Case C-45/07, ECLI:EU:C:2009:81 and Judgment in *Commission v. Sweden*, Case C-246/07, ECLI:EU:C:2010:203.

[16] See the Explanations to the Charter, available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF (last accessed 3 November 2014).

generally, in light of the explanations to Article 8, it is difficult to understand how the Directive itself could be challenged as incompatible with Article 8 of the Charter.

(iv) In this regard, it should be noted that the Directive itself is limited in its application to matters of national security. Article 3(2) confirms that the Directive shall not apply to the processing of personal data *inter alia* "in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law".[17] A similar limitation exists under Annex I of the Commission Decision, which confirms that adherence to the Safe Harbour Privacy Principles may be limited *inter alia* "(a) to the extent necessary to meet national security, public interest, or law enforcement requirements" and "(b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization". The protection of personal data in a national security context does not fall within the scope of the Directive and is only partly addressed in the Commission Decision.

(v) In assessing the validity of the Directive and the Commission Decision and the proportionality of any limitation on Articles 7 and 8 of the Charter, regard must be had, in particular, to the safeguards enshrined in the Directive and in the Commission Decision, particularly in Annex I thereof which sets out the Safe Harbour Privacy Principles, including the principle of enforcement. In addition to the enforcement mechanisms referred to in Annex I, as discussed above, independent national authorities, including the Data Protection Commissioner in the case of Ireland, may in

[17] See also Recital 13 to the Directive.

appropriate cases investigate complaints of non-compliance of transfers with the adequate level of protection required under Article 25 of the Directive.

D. Conclusions

40. FOR THESE REASONS it is submitted that the Court should respond as follows to the Reference for preliminary ruling from the High Court (Ireland) made on 25 July 2014:

> In the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC). However, the office holder may conduct his or her own investigation of such complaints in appropriate cases, in particular under Article 3(1) of the Commission Decision.

Dated the 6th day of November 2014

Signed: Tony Joyce

Agent for Ireland

on behalf of Eileen Creedon, Chief State Solicitor.

Signed: Brendan Counihan

Agent for Ireland

on behalf of Eileen Creedon, Chief State Solicitor.